



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/606,089	06/25/2003	Brian S. Christian	303956.01	4285
69316 7590 10/06/2010 MICROSOFT CORPORATION ONE MICROSOFT WAY REDMOND, WA 98052				
EXAMINER WILLIAMS, JEFFERY L.				
ART UNIT		PAPER NUMBER		
2437				
NOTIFICATION DATE		DELIVERY MODE		
10/06/2010		ELECTRONIC		

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

DBOUTON@MICROSOFT.COM  
vfiling@microsoft.com  
stevensp@microsoft.com

# Office Action Summary

**Application No.**

10/606,089

**Applicant(s)**

CHRISTIAN ET AL.

**Examiner**

JEFFERY WILLIAMS

**Art Unit**

2437

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 23 September 2010.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1,4-12, 16-21 and 24-28 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1,4-12, 16-21, 24-28 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB06)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_

**DETAILED ACTION**

This action is in response to the communication filed on 9/23/10.

All objections and rejections not set forth below have been withdrawn.

Claims 1, 4-12, 16-21, and 24-28 are pending.

***Continued Examination Under 37 CFR 1.114***

A request for continued examination under 37 CFR 1.114 was filed in this application after a decision by the Board of Patent Appeals and Interferences, but before the filing of a Notice of Appeal to the Court of Appeals for the Federal Circuit or the commencement of a civil action. Since this application is eligible for continued examination under 37 CFR 1.114 and the fee set forth in 37 CFR 1.17(e) has been timely paid, the appeal has been withdrawn pursuant to 37 CFR 1.114 and prosecution in this application has been reopened pursuant to 37 CFR 1.114. Applicant's submission filed on 9/23/10 has been entered.

***Claim Rejections - 35 USC § 101***

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

**Claims 1, 4-12, 16-21, and 24-28 rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.**

Regarding claims 1 and 4 – 11, the applicant recites a method failing to be tied to a particular machine or cause the transformation of matter into another state or thing and thus fails to recite a method falling within the scope of statutory subject matter. It is noted that the recitation of "a computing device" appears to comprise the disclosed entities such as web services ,servers, browsers, and clients that are seen to be software entities in and of themselves are they are not necessarily stated or claimed to be embodied in hardware structure (e.g. see fig. 1:102). The examiner respectfully suggests that the applicant explicitly recite hardware structure within the claim. Furthermore, the recitation of "embodied on computer storage media" does not appear to preclude the use of signals which can be used to embody (i.e. "store") software instructions (e.g. see par. 72). The examiner respectfully suggests that the applicant recite "embodied on *non-transitory* computer storage media".

Regarding claims 12, 16 – 21, and 24 - 28, the applicant recites a system comprising software embodied upon signals and media bearing instructions. The recitation of "embodied on computer storage media" (e.g. claim 1, 12) does not appear to preclude the use of signals which can be used to embody (i.e. "store") software instructions (e.g. see par. 72). As software embodied upon signals fails to comprise statutory subject matter, these claims are rejected as non-statutory. The examiner

respectfully suggests that the applicant recite "embodied on *non-transitory* computer storage media".

***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

**Claims 1, 4-12, 16-21, and 24-28 are rejected under 35 U.S.C. 102(b) as being anticipated by Scott et al. (Scott), "Abstracting Application-Level Web Security".**

Regarding claim 1, Scott discloses:

*receiving data input through a web page from a client device (fig. 1, page 2, col. 1, par. 3-6); referencing a declarative module to determine a client input security screen to apply to the data input from the client device (page 3, col. 2, par. 2);*

*wherein the declarative module comprises:*

*a global section that includes at least one client input security screen that applies to any type of client input value (fig. 2; page 6, col. 1, par. 1, 2, par. 2, lines 9-13). Scott discloses input security screens (i.e. a transformation screen) that are applied to all user input (parameters values);*

1            *an individual values section that includes at least one client input security screen*  
2            *that applies to a particular type of client input value* (fig. 2; page 4, col. 1). Herein, Scott  
3            discloses screens for screening particular types of client input values (i.e. cookies, urls,  
4            other parameters). Thus Scott discloses an individual values section.

5            *and applying multiple client input security screens to the data input from the client*  
6            *device* (page 3, col. 2, par. 2; fig. 2), *including at least one client input security screen*  
7            *from the global section of the declarative module and at least one client input security*  
8            *screen from the individual values section of the declarative module, wherein the client*  
9            *input security screens are distinct from one another* (page 3, col. 2, par. 1, 2; fig. 2).

10          Herein, Scott discloses separate screens.

11          *and wherein said act of referencing comprises first using the global section to*  
12          *screen one or more client input values and then using the individual values section to*  
13          *screen at least one of said one or more client input values* (sect. 3.4, par. 3).

14  
15          Regarding claim 4, Scott discloses:

16          *wherein the particular type of client input value is one of the following types of*  
17          *client input values: query string; server variable; form value; cookie* (Scott, fig. 2).

18  
19          Regarding claim 5, Scott discloses:

20          *wherein the declarative module further comprises a web.config file* (Scott, page  
21          1, col. 2, par.3; page 3, col. 2, par. 1).

22

Regarding claim 6, Scott discloses:

*wherein the applying the client input security screen further comprises executing a default action on invalid client input detected by the client input security screen* (Scott, page 3, col. 2, par. 1, lines 8-13, par. 2, lines 5-11; page 4, col. 2, par. 3,4). Scott discloses the application of several types of input screening to all input data (default screening) wherein actions are performed on the all the input data during the process of data input security screening. Additionally, Scott discloses default transformations that can be applied during the screening of invalid input data.

Regarding claim 7, Scott discloses:

*wherein the applying the client input security screen further comprises executing a specified action on invalid client input detected by the client input security screen, the specified action being specified in the client input security screen* (Scott, page 4, col. 1, par. 4-6).

Regarding claim 8, Scott discloses:

*wherein a client input security screen further comprises one or more values that may be entered as client input, the one or more values further comprising the only values that may be entered as client input* (Scott, page 4, col. 1, par. 4-6). Scott discloses a security screen that constrains client input to a set of values, such as any integer:  $0 - \text{int}[\text{length } 4]$ . Thus, the security screen effectively comprises the values of  $0 - \text{int}[\text{length } 4]$  to be imposed upon the client input as a restriction. Additionally, Scott

discloses that the security screen comprises specific URL values (extracted from HTTP requests) that may be entered as client input (Scott, page 6, col. 2, par. 1).

Regarding claim 9, Scott discloses:  
*wherein a client input security screen further comprises one or more screened values that, when detected in the client input, cause an action to be taken on the client input* (Scott, fig. 4; page 3, col. 2, par. 2; page 4, col. 2, par. 3).

Regarding claim 10, Scott discloses:  
*wherein the action to be taken further comprises removing the one or more screened values detected in the client input* (Scott, fig. 4; page 3, col. 2, par. 2; page 4, col. 2, par. 3, 4). Scott discloses the encoding of screened values (removal and replacement). Additionally, Scott discloses the removal of values from client input based upon the client input security screen (Scott, page 7, col. 2, par. 1.1 – 1.2)

Regarding claim 11, Scott discloses:  
*wherein the action to be taken further comprises removing an entire string that contains the one or more screened values detected in the client input* (Scott, page 6, col. 2, par. 3; fig. 5; page 9, col. 1, par. 2.2).



Regarding claim 12, it is the system claim corresponding to the method claim 1, and is rejected for, at least, the same reasons, and furthermore because Scott discloses:

*a web page server unit configured to provide one or more web pages to one or more client devices over a distributed network (Scott, fig. 1).*

Regarding claim 16, Scott discloses:

*wherein a screening rule further comprises a client input variable that may be accepted as input from a client (Scott, fig. 5).* Scott discloses various screening rules that accept client input variables.

Regarding claim 17, Scott discloses:

*wherein a screening rule further comprises one or more screened characters that, when detected in client input, are screened from the client input according to a screening rule (Scott, fig. 5 – see transformation).*

Regarding claim 18, Scott discloses:

*wherein the screening rule further comprises a default screening action that is applied in the absence of a specified screening action (Scott, fig. 5 – see transformation).* Scott discloses a single screening action that is to be performed, and thus, a default screening action.

Regarding claim 19, Scott discloses:

*wherein the screening rule further comprises a specified screening action that is applied to the screened client input* (Scott, fig. 5 – see transformation). Scott discloses a single specific screening action that is to be performed.

Regarding claim 20, it is rejected, at least, for the same reasons as claim 5.

Regarding claim 21, it is rejected, at least, for the same reasons as claim 1, and furthermore because Scott discloses:

*serving a web page to a client over a distributed network; receiving client input via the web page* (Scott, fig. 1, page 2, col. 1, par. 3-6); *comparing the client input with multiple and distinct client input security screens stored in a security declarative module; wherein the security declarative module includes a global section configured to screen all types of client input values and an individual values section configured to screen particular types of client input values* (see rejection of claim 1); *if invalid client input is detected, performing a screening action on the invalid client input as indicated by the security declarative module* (Scott, page 3, col. 2, par. 2; page 4, col. 2, par. 3; page 6, col. 1, par. 1, 2; fig. 5); *and wherein the client input security screens included in the security declarative module can be applied to multiple web pages* (Scott, page 4, col. 1, par. 2).

Furthermore, Scott discloses a computer system, and thus discloses media and instructions (Scott, fig. 1).

Regarding claims 24 and 25, they are the media and instruction claims corresponding to the method and system claims of 5 – 7, 18, and 19, and they are rejected for, at least, the same reasons.

Regarding claim 26, Scott discloses:  
*wherein the screening action further comprises a default action that is not required to be specified in a client input security screen* (Scott, page 6, col. 1, par. 1, 2).

Regarding claims 27 and 28, Scott discloses:  
*wherein the multiple web pages are included in a web project and wherein the multiple web pages are included in a web-based application* (Scott, Abstract; Introduction; fig. 1; section 3.1; page 4, col. 1, par. 2; page 6, col. 1, par. 2, col. 2, par. 1). Scott discloses a security policy to be applied to a large web-application, the policy comprising rules for the web pages of a site. The web pages are associated with a web application, thus, they are included in a web project/application.

### ***Response to Arguments***

Furthermore, Applicant's arguments filed 9/23/10 have been fully considered but they are not persuasive.

*Applicants argue or assert essentially that:*

The Board states that "[t]o the extent recited in the claims, the web services, servers, browsers, and clients appear to be software entities in and of themselves and they are not necessarily stated or claimed to be embodied in hardware structure" (Decision on Appeal, pg. 5). Applicant respectfully points out that claim 1 recites "a client device" which is described in the Specification, among other places on pg. 12, lines 21-22: "[c]omputer environment 400 includes a general-purpose computing device in the form of a computer 402. Computer 402 can be, for example, a client 110 or server 102". Accordingly, a client device is indeed a statutory hardware device.

(Remarks, pg. 10)

*Examiner respectfully responds:*

It is respectfully noted that the examiner agrees with the findings of the Board. Particularly, the applicant's recitation of "a computing device" appears to comprise the disclosed entities such, as a server, that are seen to be software entities in and of themselves are they are not necessarily stated or claimed to be embodied in hardware structure (e.g. see fig. 1:102). Furthermore, the applicant's arguments fail to comprise evidence or rationale showing that the claims comprise any particular recitation of hardware. The examiner respectfully suggests that the applicant explicitly recite hardware structure within the claim.

*Applicants argue or assert essentially that:*

Applicant's specification describes "computer storage media" on pg. 17, lines 8-16 which is reproduced below for the convenience of the Office.

"Computer storage media" includes volatile and non-volatile, removable and non-removable media implemented in any method or technology for storage of information such as computer readable instructions, data structures, program modules, or other data. Computer storage media includes, but is not limited to, RAM, ROM, EEPROM, flash memory or other memory technology, CD-ROM, digital versatile disks (DVD) or other optical storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or any other medium which can be used to store the desired information and which can be accessed by a computer.

Computer storage media, as supported by the Specification, is indeed statutory in nature. Accordingly, for all of these reasons, Applicant respectfully requests that the § 101 rejection be withdrawn.

(Remarks, pg. 11)

*Examiner respectfully responds:*

It is respectfully noted that the examiner agrees with the findings of the Board. Particularly, it is noted that the recitation of "embodied on computer storage media" (e.g. claim 1, 12) does not appear to preclude the use of signals which can be used to embody (i.e. "store") software instructions (e.g. see par. 72). Furthermore, it is noted that the applicant's remarks comprise only a non-limiting example of "computer storage

media" and is not seen as a definition precluding the use of signals for embodying (e.g. "storing") software. As software embodied upon signals fails to comprise statutory subject matter, these claims are rejected as non-statutory. The examiner respectfully suggests that the applicant recite "embodied on *non-transitory* computer storage media".

### ***Conclusion***

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

***See Notice of References Cited.***

A shortened statutory period for reply is set to expire 3 months (not less than 90 days) from the mailing date of this communication.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffery Williams whose telephone number is (571) 272-7965. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Jeffery Williams/  
Examiner, Art Unit 2437  
  
/Emmanuel L. Moise/  
Supervisory Patent Examiner, Art Unit 2437